

Trend Micro Expands Into E-mail Archiving

Date: March, 2008

Author: Lauren Whitehouse, Analyst and Brian Babineau, Senior Analyst

Abstract: E-mail is at the core of every business as the primary means of communication and collaboration. As such, messages are now subject to record retention regulations and electronic discovery events (80% of which involve e-mail). Modifying existing backup processes for archiving is not enough to address the volume of data or new accessibility requirements. Trend Micro has entered the market with Message Archiver, an e-mail archive solution that is currently geared to help small- and medium-sized businesses (SMBs) meet the compliance and legal challenges pertaining to managing and retaining messages.

A Different Perspective in the E-mail Archive Market

If you are one of those organizations that believe compliance and electronic discovery events only happen to the big Wall Street banks, think again. E-mails are now considered business records in almost any industry; especially in SMBs using electronic messages to exchange invoices, contracts and other business-critical files. Private and public companies, government agencies and non-profit organizations must all deal with new e-mail challenges because saving messages in an accessible format for long periods of time is a business necessity.

A majority of solutions in the marketplace target large enterprise IT departments capable of running substantial e-mail archive implementations. Trend Micro has entered the e-mail archive market with a different perspective. First, as a leader in e-mail security solutions for the past 20 years, the company understands message management. Secondly, Trend Micro is aware of the challenges facing SMBs and builds solutions specifically to meet these organizations' requirements. Using this insight, the company recently introduced the Trend Micro Message Archiver.

Archives Need to Be Accessible

Organizations need to understand why current archiving processes must change. Many IT departments do not even differentiate between backup and archiving. Archiving has traditionally been a derivative of the backup process, as IT simply saves tapes for extended periods of time and calls this a "corporate archive." Before the early part of this decade, this form of archiving was satisfactory because there were hardly any reasons to access old data. Now that record retention regulations encompass e-mail and attorneys are sifting through message repositories during legal discovery events, archives need to be accessible. Things must change.

Recognizing that archiving is not synonymous with backup is a big hurdle for organizations to overcome, but it must be done and a good starting place is e-mail. Customers will soon realize the benefits of archiving messages, including reducing e-mail storage costs, expediting compliance and reducing legal expenses. With benefits like that, it is not surprising that many vendors and outsourcers now offer e-mail archive solutions.

Message Archiver at a Glance

How it Works

Message Archiver is a software solution that runs on a server within a Microsoft Exchange environment. The software receives messages from the Exchange message journal, then indexes and stores them. They are stored (on storage internal or external to the server) and retained based on a predefined policy, which is often determined by record retention regulations or legal preservation requirements. In either case, the messages cannot be altered or deleted for a specified period.

Because it integrates with Exchange's journaling capability, Message Archiver captures all messages, including those sent inside and outside of organizations. As messages enter the solution, each e-mail receives its own

digital fingerprint and is encrypted for enhanced security. The digital fingerprint will also permit Message Archiver to easily identify duplicate messages and perform single instancing (removing duplicate data before storing it). Currently, when one message is sent to multiple people, only one copy of the message and attachment is retained by Message Archiver. In the future, Message Archiver will be able to identify duplicate attachments across multiple messages. Before messages are stored, they are compressed. When combined with single instancing, Message Archiver helps control storage costs by maximizing capacity utilization while reducing the volume of data that must be searched during a legal or regulatory inquiry.

Message Archiver is designed to prevent data tampering. Digital fingerprinting helps prove the authenticity of a particular message, which assists in the chain-of custody process during legal or regulatory discovery events.

A Better Approach to Search

Message Archiver provides role-based search access because multiple constituents require different permissions when querying e-mails. The Administrator Role lets IT configure and monitor the archive software and retrieve messages sent to and from an administrative mailbox. All activities performed by an Admin are traced within the secure logs of the Message Archiver. Because corporate counsel and compliance officers often need to look through the entire archive for messages that may be responsive to a specific case, these users are assigned with the Privileged Role. Queries initiated by Privileged users return results from the entire archive. For privacy concerns, an e-mail detailing Privileged users' activities can be sent to a Data Guardian. A Data Guardian may be a union representative, an internal auditor, external counsel or other representative that should be notified if a legal or regulatory investigation is taking place. This helps ensure that Privileged users are only conducting searches that are necessary.

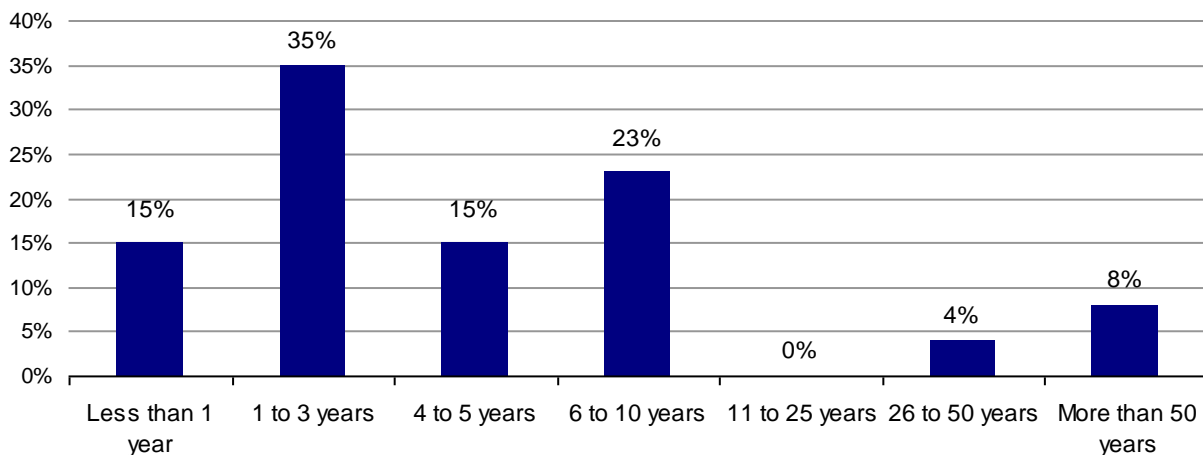
One of the main goals of an archive is to provide a central repository of messages for business reference. Authorized employees can search for their own messages. The query results only contain messages sent to or from the specific employee, ensuring that there are no privacy violations or confidential data breaches.

Using Message Archiver

Customers facing any number of challenges can benefit from the use of Message Archiver for e-mail archiving. For starters, if you currently enforce mailbox quotas, you are forcing employees to delete older messages or create personal archives. The latter can increase legal discovery costs, as attorneys have to search message systems and PCs. Some organizations save e-mails for long periods of time (Figure 1), which can increase storage costs. With Message Archiver, messages can be deleted from the primary Exchange environment based on a policy such as date or size, but are still available for access because they are centrally archived elsewhere. These messages can then be deleted when they are no longer needed for business reference and legal purposes. Additionally, when a discovery inquiry arrives, attorneys only have one place to search—which can save a significant amount of time and money.

FIGURE 1. AVERAGE LENGTH OF TIME SMB ORGANIZATIONS RETAIN ARCHIVED E-MAIL INFORMATION

To the best of your knowledge, what would you say is the average length of time that your organization retains archived e-mail information? (Percent of SMB respondents, N=26)



Source: ESG Research Report, 2007 E-mail Archiving Survey, November 2007

During an electronic discovery, attorneys need to find relevant information and properly preserve it. Customers do have choices regarding evidence preservation. Some rely on employees to manually save messages within a personal archive folder, while others keep backup tapes for the life of the case. There is risk involved with both of these approaches, as employees may purposely or accidentally delete messages. Tapes may be hard to read and expensive to restore when they are needed. Lack of proper preservation can lead regulatory bodies to impose fines (with recent penalties ranging from a \$15M fine for Morgan Stanley¹ and a \$1.5M² forced settlement for the City of Dallas). Courts can also issue an adverse opinion if evidence tampering occurs. If information is not properly preserved, it may hinder the responsible party's argument. As such, once attorneys determine the criteria—such as employees and date range—that will be responsive to an investigation or matter, Message Archiver can provide all the messages that meet these specifications, and will capture additional relevant e-mails. Once inside Message Archiver, the messages cannot be deleted by any unauthorized user.

With some organizations keeping messages for up to ten years, it is imperative that they are saved efficiently and cost effectively. Message Archiver facilitates compliance with record retention regulations such as HIPAA, SEC Rules 17a-3 & 4 and Financial Services Authority (UK). Even local governments are establishing rules like New South Wales' (Australia) government policies on digital records retention preservation.³ All e-mails are captured—from one employee or a group of mailboxes—and retained. Customers can leverage Message Archiver's integration with Active Directory and LDAP to authenticate user access to archived messages. The messages remain online and searchable for the appropriate retention periods. Electronic records management programs are also being driven by the increased focus on corporate governance. Message Archiver makes it simple to expand these programs to e-mail.

The Bottom Line

There are plenty of reasons why organizations should adopt e-mail archiving, yet to date; only highly-regulated enterprises have taken the leap. It's true that many of these organizations didn't have a choice—e-mails were quickly amalgamated into record retention regulations and immediately, litigators began targeting messages as key sources of evidence. These trends have led to the misconception that only enterprises need e-mail archive

¹ <http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,108687,00.html>

² http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/DN-gamez_28met.ART.West.Edition1.438a407.html

³ http://www.records.nsw.gov.au/recordkeeping/policy_on_digital_records_pres_14381.aspboolean

solutions because they are the only ones subject to discovery requests or because they have the resources to deploy electronic records management programs—which is not actually the case.

Two big things have been missed while most of the market has focused solely on enterprise e-mail archives. First, additional benefits of e-mail archives—such as the enforcement of mailbox quotas without requiring employees delete messages or create personal folders—are often overlooked,. Secondly, SMBs face the same discovery, regulatory and quota management issues as their enterprise brethren. The biggest difference between SMBs and enterprises is that SMBs need a solution that is easy to install and operate because they do not have enough IT resources to run anything more.

There's always room for improvement. Message Archiver currently supports Microsoft Exchange, but many shops run Lotus Notes or other Linux-based e-mail packages. The solution is being introduced in the form of software, requiring the customer to buy and deploy a server based on the specifications published by Trend Micro. To ease the whole process for customers, Trend Micro should consider an appliance (or a virtual appliance—based on VMware) approach where the Message Archiver software is preloaded onto a server, making it easier to install. However, these drawbacks pale in comparison to the potential benefits a customer can achieve with an e-mail archive solution such as Trend Micro's Message Archiver.